BURSOR & FISHER, P.A.
L. Timothy Fisher (State Bar No. 191626)
Stefan Bogdanovich (State Bar No. 324525)
1990 North California Blvd., Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: ltfisher@bursor.com
sbogdanovich@bursor.com

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA—EASTERN DIVSION

ISIAH SHEPPARD, HILSCIO RIVERA, HELENE LAUZIER-MEYER, and BERNABE BENITEZ, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

FANTASIA TRADING LLC, d/b/a EUFY,

Defendant.

Case No. 5:23-cv-02407-JGB-E

FIRST AMENDED CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs Isiah Sheppard, Hilscio Rivera, Helene Lauzier-Meyer, and Bernabe Benitez ("Plaintiffs") bring this action on behalf of themselves and all others similarly situated against Defendant Fantasia Trading LLC, d/b/a Eufy ("Defendant" or "Eufy") for violations of Illinois' Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1, *et seq.* The following allegations are based on their counsel's investigation and upon information and belief, except for allegations concerning Plaintiffs themselves, which are based on personal knowledge.

NATURE OF THE ACTION

1. Plaintiffs bring this action for damages and other legal and equitable remedies resulting from the illegal actions of Defendant in collecting and storing their and other similarly situated individuals' biometric identifiers without first obtaining informed written consent and failing to develop, maintain, or much less provide a data retention and destruction schedule, in direct violation of BIPA.

2. The Illinois Legislature has found that "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information." 740 ILCS 14/5(c). "For example, social security numbers, when compromised can be changed. Biometric identifiers, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identify theft, and is likely to withdraw from biometric-facilitated transactions." *Id.*

3. In recognition of these concerns over the security of individuals' biometric identifiers, the Illinois Legislature enacted BIPA, which provides, *inter alia*, that a private entity like Defendant may not obtain and/or possess an individual's biometric identifiers unless it informs that person in writing that biometric identifiers or information will be collected or stored. *See* 740 ILCS 14/15(b).

4. Likewise, BIPA also requires that entities collecting biometric identifiers must publish and make publicly available written retention schedules and

guidelines for permanently destroying biometric identifiers collected. *See* 740 ILCS 14/15(a).

5. In direct violation of each of the foregoing provisions of §§ 15(b) and 15(a) of BIPA, Defendant collected, stored, and used—without providing notice, obtaining informed written consent and without publishing a data retention schedule—the biometric identifiers of Illinois delivery drivers making deliveries to homes using Defendant's home security system.

6. To be sure, the BIPA independently prohibits the unconsented collection of biometric identifiers that can be used to distinguish unique individuals. Nothing in the text or the history of the statute gives Defendant a free pass to collect this sensitive data without people's consent simply because a Defendant avoids actively using the biometric identifiers it collects to identify individuals, or avoids collecting those same individuals' names, addresses, or other information to link those biometric identifiers back to their real-world identifies.

7. BIPA confers on Plaintiffs, and all those similarly situated Illinois residents who make home deliveries, the right to know of such risks, which are inherently presented by the collection and storage of their biometric identifiers. Plaintiffs also have a right to know how long such risks will persist while their biometric identifiers are stored and used by Eufy's AI, which, once collected and stored, scans biometric identifiers to create mechanical measurements necessary for identifying and differentiating specific shapes, objects, and people.

8. This is particularly concerning because other home security companies like Google Nest and Wyze do not allow their cameras and doorbells with facial recognition capabilities to be used in Illinois.[1]

[1] Google Store, *Nest Aware*, available at https://store.google.com/us/product/nest_aware?hl=en-US&pli=1 (last accessed Oct. 18, 2023); Wyze, *How do I set up Friendly Faces?* (July 21, 2023), available at https://support.wyze.com/hc/en-us/articles/5876322908315-How-do-I-set-up-Friendly-Faces- (last accessed Oct. 18, 2023).

9. Plaintiffs bring this action to prevent Defendant from further violating the privacy rights of Illinois delivery drivers and to recover statutory damages for Defendant's unauthorized collection, storage, and use of their biometric identifiers in violation of BIPA.

PARTIES

10. Plaintiff Isiah Sheppard is a resident of Cook County, Illinois. Plaintiff Sheppard works as an Uber Eats and DoorDash delivery driver who makes deliveries to customers' homes. As part of Plaintiff Sheppard's regular deliveries process, he walks to the front door of the customer's residence to make the delivery. On multiple deliveries, scans of Plaintiff Sheppard's face and/or hands were captured by Defendant's security system. Plaintiff Sheppard has a publicly available Facebook account searchable by his name and which features photos of himself.

11. Plaintiff Hilscio Rivera is a resident of Cook County, Illinois. Plaintiff Rivera works as an Amazon, DoorDash, Postmates, Dispatch, Veho, AxleHire and Roadie delivery driver who makes deliveries to customers' homes. As part of Plaintiff Rivera's regular delivery process, Plaintiff Rivera walks to the front door of the customer's residence to make the delivery. On multiple deliveries, scans of Plaintiff Rivera's face and/or hands were captured by Defendant's security system. Plaintiff Rivera has a publicly available Facebook and Twitter accounts, searchable by his name and which feature photos of himself.

12. Plaintiff Helene Lauzier-Meyer is a resident of Sangamon County, Illinois. Plaintiff Lauzier-Meyer works as a DoorDash and Spark delivery driver who makes deliveries to customers' homes. As part of Plaintiff Lauzier-Meyer's regular deliveries process, she walks to the front door of the customer's residence to make the delivery. On multiple occasions, scans of Plaintiff Lauzier-Meyer's face and/or hands were captured by Defendant's security system. Plaintiff Lauzier-Meyer has a publicly available Facebook account searchable by her maiden name and which feature images of herself.

13. Plaintiff Bernabe Benitez is a resident of Lake County, Illinois. Plaintiff Benitez works as an UberEats delivery driver who makes deliveries to customers' homes. As part of Plaintiff Benitez's regular deliveries process, he walks to the front door of the customer's residence to make the delivery. On multiple occasions, scans of Plaintiff Benitez's face and/or hands were captured by Defendant's security system. Plaintiff Benitez has publicly available Facebook and TikTok accounts searchable by his last name and which feature images of himself.

14. Defendant Fantasia Trading LLC is a Delaware corporation with its principal place of business in Ontario, California. Fantasia Trading LLC is the parent company of Anker Innovations and Eufy.

15. Eufy is a home security technology company that offers security cameras supported by high quality video and artificial intelligence ("AI") monitoring.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) because there are more than 100 class members and the aggregate amount in controversy exceeds $5,000,000.00, exclusive of interest, fees, and costs, and at least one class member is a citizen of a state different from Defendant.

17. This Court has personal jurisdiction over Defendant because Defendant has its principal place of business in this district, in Ontario, California.

18. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendant is at home in this District.

FACTUAL ALLEGATIONS

I. Eufy's Home Security System, Local AI and BionicMind AI.

19. Eufy is an emerging leader in home security systems. However, Eufy "isn't like your traditional alarm company. It's a tech company first[.]"[2]

20. To that end, Eufy sells 36 different security camera models, each equipped with on-device AI monitoring capabilities.[3] These cameras include multiple models of doorbell cameras, exterior mounted and floodlight cameras, and a series of base stations.[4]

21. Eufy's AI technology is categorized as either "Local AI" or "BionicMind AI." Together, they offer homeowners several different detection features depending on the user's subscription and base station.

22. "Local AI" (Eufy's on-device AI mechanism) uses an "embedded AI chip" built into the cameras which provides "local, safe, and intelligent detection."[5]

23. The "BionicMind AI" system "has the ability to recognize similar faces, body shapes/positions, different objects, and even human behavior with its machine self-learning system."[6] The system conducts this analysis "locally on the base station"[7] and is added to an already operating Eufy system by incorporating the proper base station.

---

[2] Aliza Vigderman & Gabe Turner, *Eufy Security System Review and Cost*, Security.org (Oct. 12, 2023) *available* https://www.security.org/home-security-systems/eufy/ (last accessed Oct. 18, 2023).

[3] Eufy, *AI Features for eufySecurity Devices*, available https://support.eufy.com/s/article/AI-Features-for-eufySecurity-Devices (last accessed Oct. 18, 2023).

[4] *Id.*

[5] *Id.*

[6] Jared Locke, *Eufy's Latest Edge Security System Features Self-Learning AI to Identify Family and Friands*, 9To5 Toys (Sep. 30, 2022) *available* https://9to5toys.com/2022/09/30/eufy-edge-security-system-launch/ (last accessed Oct. 23, 2023).

[7] *Id.*

24. Eufy's intelligent detection arises through six unique features: (1) a human detection feature where the system tries "to detect objects similar to the human shape and filter out other objects like cars and animals for motion alerts;" (2) facial detection where the system tries to "detect and screen faces shown in the video image;" (3) human facial recognition where the system tries to "recognize faces in the video image and identify the person for [the homeowner];" (4) pet detection where the system tries "to detect pets which appear in the video image;" (5) crying detection where the system tries "to detect crying and will notify [the homeowner] if necessary;" and (6) vehicle detection where the system "will catch up with the user's vehicle in the backyard or driveway."[8]

25. Generally, the kind of base station the homeowner uses impacts which version of Eufy's AI the homeowner can turn on. For example, the base level "Original HomeBase" allows all AI-incorporated cameras and battery-operated video doorbells to use the human detection and facial recognition features. The "HomeBase 3", alternatively, allows the homeowner to deploy each AI recognition feature. "HomeBase E" and "HomeBase 2" allow the homeowner to use just the Human Detection and Facial Recognition detection features.[9]

26. Although the homeowner has, in some instances, a choice of *which* base station to pair with their Eufy camera, "eufyCam (eufyCam [,] eufyCam E [,] eufyCam 2 [,] eufyCam 2C [,] eufyCam 2 Pro [,] eufyCam 2C Pro) *must* be used with HomeBase[,]"[10] thereby ensuring that EufyCam and EufyCam2 cameras are AI-capable. Likewise, the EufyCam 3 comes included with the HomeBase3.[11]

---

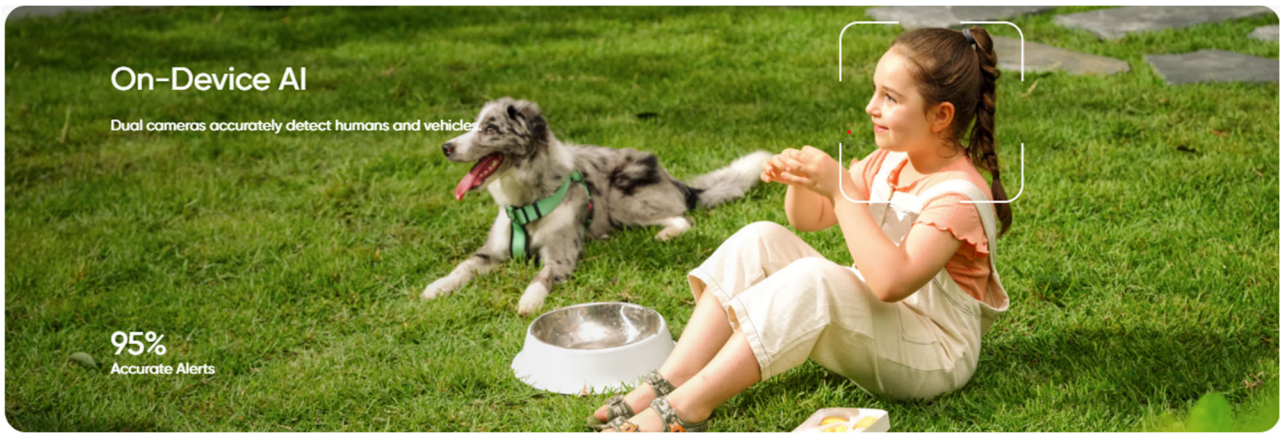
[8] Eufy, *supra* note 3.

[9] *Id*.

[10] Eufy, *Does eufyCam Have to be Used with HomeBase?* available https://support.eufy.com/s/article/Does-eufy-cameras-have-to-be-used-with-HomeBase (last accessed Feb. 1, 2024) (emphasis added).

[11] Cool Blue, *What are the Differences Between the EufyCam 3, 2 Pro, and 2?* available https://www.coolblue.nl/en/advice/compare-the-eufycam-3-with-the-2-pro-and-2.html (last accessed Feb. 1, 2024).

27. However, unlike the rest, Eufy's *wired* video doorbells allow the homeowner to use the human and facial detection features without needing a base station.[12]



28. Regardless of which camera is used, Eufy's Local AI system is remarkably accurate. As Eufy boasts, its on-camera AI human detection feature "accurately detect[s] humans and vehicles" 95% of the time.[13]

29. Likewise, users can enhance their system's AI capabilities by adding Eufy's BionicMind AI-equipped base stations to their security systems.[14] Eufy's BionicMind AI system, which can be added simply by connecting a new base station,[15] "uses self-learning algorithms after every facial and body shape scan to

---

[12] Eufy, *supra* note 3.

[13] Eufy, *SoloCam S340*, available https://www.eufy.com/solocam-s340?utm_source=google&utm_medium=search&utm_content=alwayson&utm_campaign=us_security_edge_conversion_search_eufycam_purchase_ost_M3_bb&utm_term=19626718763_144313519606_676641948951&gclid=CjwKCAjwvrOpBhBdEiwAR58-3NdpFPlGlnThHvpGuSIhMB31i0N0GkYya92NvW0IIXAjSnobXtGefBoCVVoQAvD_BwE (last accessed Oct. 19, 2023).

[14] *See* Jennifer Pattison Tuohy, *Eufy's Impressive New Smart Cameras Use AI to Identify You and Your Pets*, The Verge (Sep. 30, 2022) *available* https://www.theverge.com/2022/9/29/23378472/eufy-homebase-3-eufycam-3-price-release-date-specs (last accessed Oct. 20, 2023).

[15] *See Id.* ("HomeBase 3 has expandable local storage up to 16 TB, while adding the power of BionicMind for an accurate AI experience.")

improve recognition accuracy to more than 99.9% over time—no matter what [the subject is] wearing and how [the subject] approach[es] the camera."[16]

30. Human detection, available for "Local AI" and "BionicMind AI" users, "detects and captures motion . . . for accurate object classification."[17] The technology "works in two steps[.]"[18] First, "[w]hen the camera detects motion in its field of view, the AI engine analyzes the figure to determine if it is a human being or not."[19] Second, "if the captured face meets the AI engine's analysis parameters, the AI engine will try to capture the face and then send a notification to the user."[20] This step allows the system to use the captured biometric identifiers in two scenarios.

---

[16] Eufy, *eufyCam 3*, *available* https://us.eufy.com/pages/security-eufycam3 (last accessed Oct. 19, 2023).

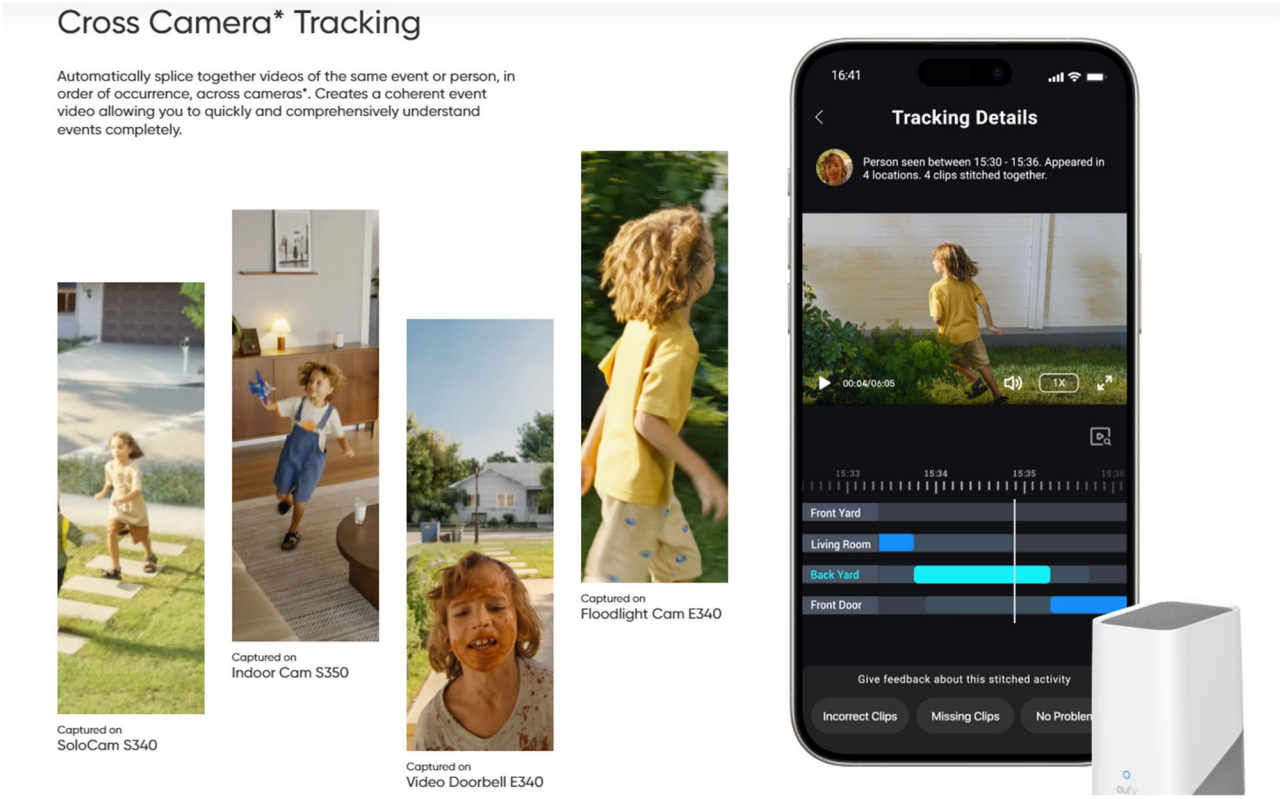
[17] Eufy, *How Does the Human Detection Technology Work?* available https://support.eufy.com/s/article/How-does-the-Human-Detection-technology-work (last accessed Oct. 19, 2023).

[18] *Id.*

[19] *Id.*

[20] *Id.*

31. One such feature is "cross camera tracking" where, once stored with the proper base station connected, Eufy's system will "automatically compile shots **of the same event and person** and organize them chronologically into a single clip"[21] if an event occurs within the view of multiple cameras.

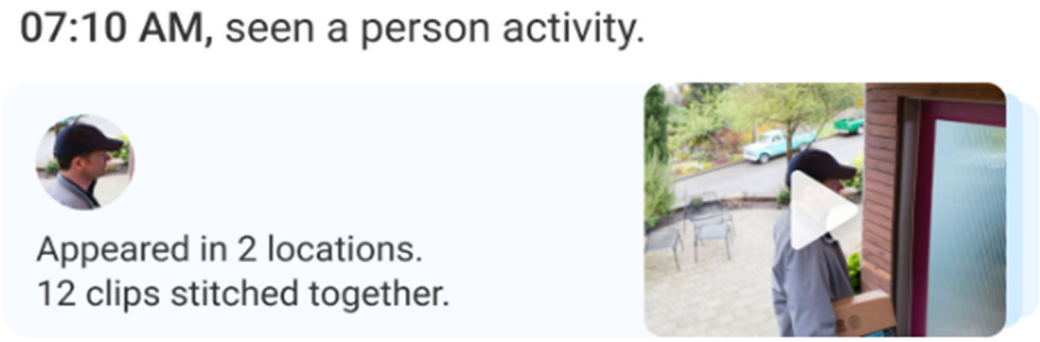


[21] Anthony Spadafora, *Eufy's New Security Cameras Use AI for Cross-Camera Tracking—Here's How it Works*, Yahoo! Finance (Sep. 26, 2023) *available*

32. As Eufy explains, "[w]hen the same individual appears across multiple cameras within a specified timeframe, the system automatically locates and merges these footage [sic] into a single video" so that the homeowner can "easily review the entire activity **of that specific individual** in a single video."[22]

33. To piece the footage together, the BionicMind base station "analyzes the video content and stitches it together in-real [sic]" time and, "[a]fter each camera has finished recording and saving videos to [the base station], [] re-analyzes the video content for splicing."[23] Cameras that are not compatible with BionicMind base stations cannot stitch images together in real time and, instead, analyze saved video after recording has ended.[24]

34. The homeowner then receives a notification alerting them that the device has either detected an already cataloged face like a friend or a new, unknown visitor like a delivery driver:

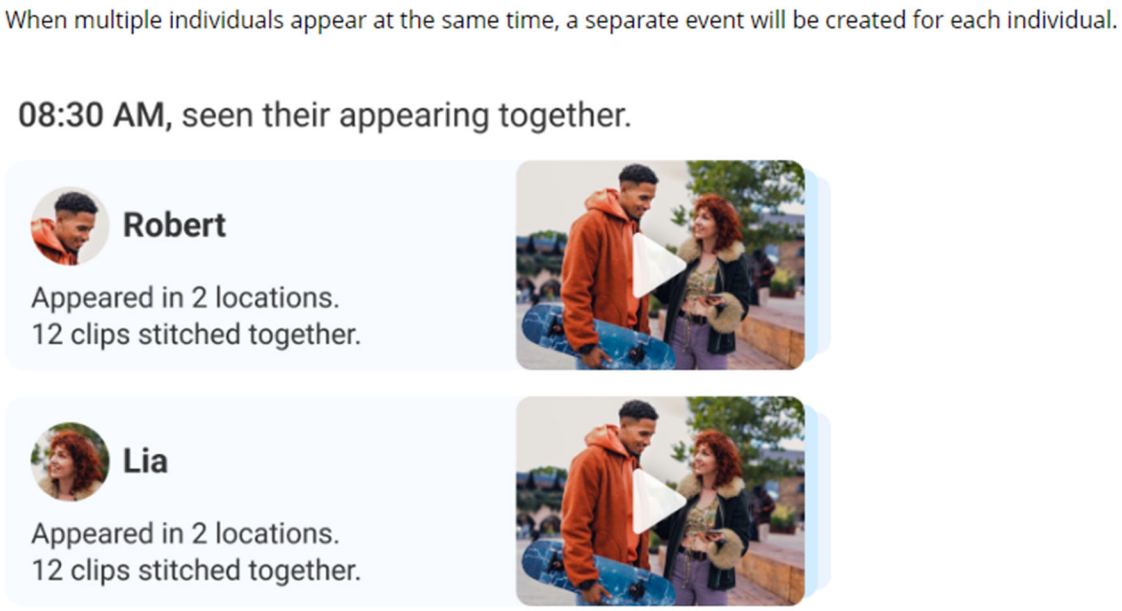


https://finance.yahoo.com/news/eufy-security-cameras-ai-cross-230048637.html. (emphasis added).

[22] Eufy Support, *Introducing the Cross-Camera Tracking Function in the Eufy Security App*, Eufy *available* https://support.eufy.com/s/article/Introducing-the-Cross-Camera-Tracking-Function-in-the-eufy-Security-App (last accessed Oct. 20, 2023) (emphasis added).

[23] *Id.*

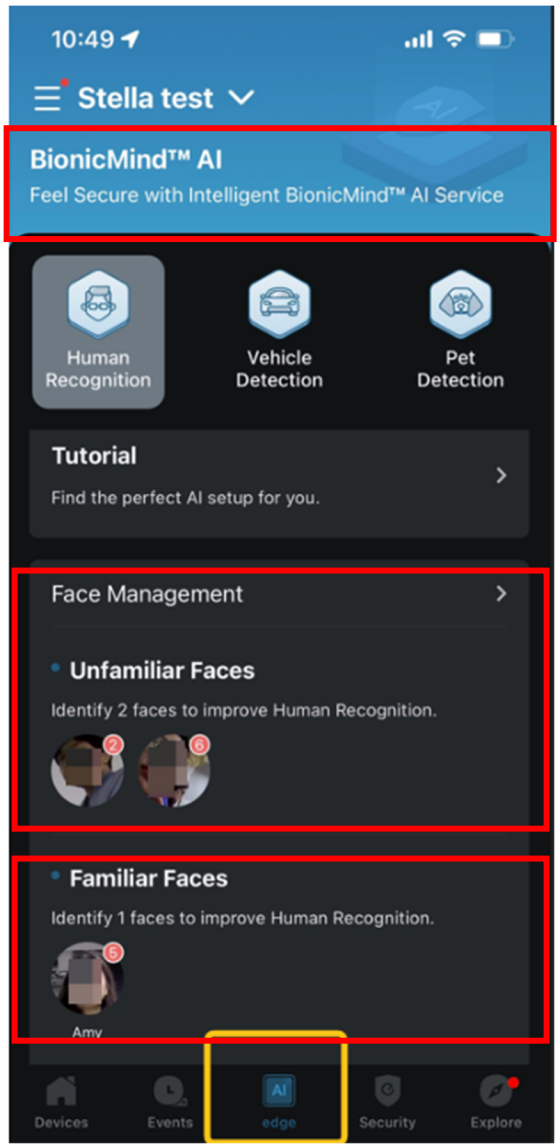
[24] *See Id.* ("Cameras that are compatible with HomeBase 3 storage, but not with HomeBase 3 BionicMind [] A.I., will only be able to use the Look-Back Tracking Function. . .").

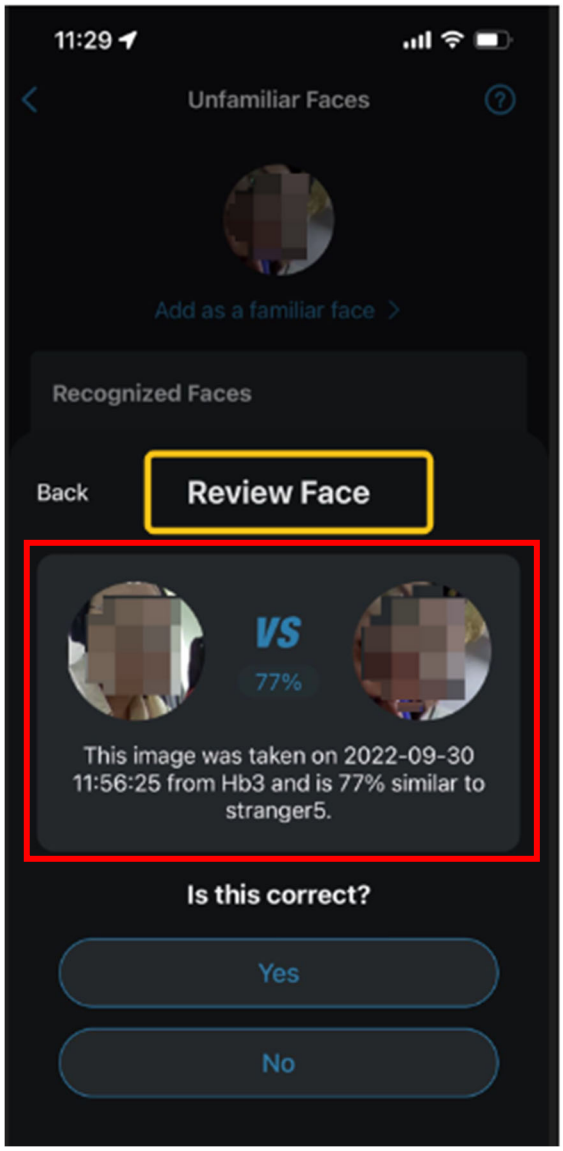


35. Eufy is capable of making these identifications by storing and analyzing biometric-identifier data so the AI can "keep learning the details of the characteristics of people, including different angles of the face and bodies" to "help the AI recognize a person more accurately and quickly."[25] That data is then accessible to the user via the EufySecurity App.[26]

[25] Eufy Support, *What is the self-learning AI in the HomeBase 3?* Eufy (Dec. 1, 2022) *available* https://support.myeufy.com.au/support/solutions/articles/73000597074-what-is-the-self-learning-ai-in-homebase-3- (last accessed Oct. 19, 2023).

[26] *Id.*





36. Eufy readily admits that "[t]he Cross-Camera Tracking function depends on a human feature recognition algorithm [sic] that determines the similarity of an individual's appearance in two videos to stitch them together. Even if the face is not visible in the video, videos of similar-looking individuals are still identified and stitched together."[27]

37. And, although Eufy represents that its AI and biometric collections are stored locally, as recently as December 2022 (well within BIPA's five-year statute of

[27] Eufy, *supra* note 25.

limitations from the commencement of this action), "it was revealed that … Eufy was sending data from its cameras to the cloud, despite … advertising its cameras and video doorbells [used] local-only recording … [after] a security researcher found that the company was uploading images from the cameras to AWS servers alongside facial recognition data."[28] Specifically, the researcher, in testing one of Eufy's devices, found that "[t]he doorbell's camera was uploading facial recognition data from the camera to Eufy's cloud servers with identifiable information attached, and that this data wasn't actually removed from Eufy's servers when the related footage had been deleted from the Eufy app."[29] The researcher, in making this discovery, also expressed concern that "Eufy could link footage collected from different cameras and apps to individuals using facial recognition."[30]

38. AWS Servers are servers offered by Amazon.com to companies like Defendant as "low-cost ways to deliver their websites and web applications" to users.[31]

39. In fact, once this and other reckless data management practices were discovered (discussed below) Eufy acknowledged in a January 2023 press release

---

[28] Ben Schoon, *Eufy Will Add a Disclosure to its App Following Security Concerns but Still Denies Glaring Security Holes,* 9to5Google (Dec. 5, 2022) *available* https://9to5google.com/2022/12/05/eufy-disclosure-cloud/ (last accessed Jan. 30, 2024).

[29] Ben Schoon, *Eufy Caught Lying About Local-Only Security Cameras with Footage Sent to Cloud, Accessible in Unencrypted Streams*, 9to5Google (Dec. 1, 2022) *available* https://9to5google.com/2022/12/01/eufy-camera-cloud-security-leak/ (last accessed Jan. 30, 2024).

[30] Joel R. McConvey, *Eufy Doorbell Cameras Uploading Facial Recognition Data to the Cloud Without Consent*, Biometric Update (Nov. 30, 2022) *available* https://www.biometricupdate.com/202211/eufy-doorbell-cameras-uploading-facial-recognition-data-to-the-cloud-without-consent (last accessed Feb. 1, 2024).

[31] *See* Amazon Web Service, *AWS*, available https://aws.amazon.com/free/webapps/?gclid=Cj0KCQiA2eKtBhDcARIsAEGTG42H9ebgefFKYVCD5h-YNFJ39VpoUAvyk1r0DUwhVMIM-iwBVJph6noaAsOaEALw_wcB&trk=0859629e-29af-428f-ab68-152ecf240a0b&sc_channel=ps&ef_id=Cj0KCQiA2eKtBhDcARIsAEGTG42H9ebgefFKYVCD5h-YNFJ39VpoUAvykIr0DUwhVMIM-iwBVJph6noaAsOaEALw_wcB:G:s&s_kwcid=AL!4422!3!531871356653!p!!g!!aws%20web%20hosting!11086666988!11T455470529 (last accessed Jan. 30, 2024).

that "[p]reviously, we [had] one device, the Video Doorbell Dual, that sent and stored an image of the user to our secure cloud. … First, the purpose of sending a user image from the eufy App to our devices is to give the local facial recognition software a baseline to run its algorithm."[32]

40. Concerningly, Eufy's data collection and storage systems were scrutinized further because of their vulnerability in storing and protecting Eufy customer and recording data. Until recently, Eufy's storage procedures placed Plaintiffs' and Class Members' biometric identifiers at risk in precisely the manner the Illinois Legislature enacted BIPA to prevent.

41. Again, in late 2022, technology reporters and security experts "accused … Eufy of lying to users that their video streams were end-to-end encrypted, even though users were easily able to access the streams using simple browser tools and a desktop media player."[33]

42. As data and technology giant Cisco explains, encryption is "the process of converting or scrambling data and information into an unreadable, encoded version that can only be read with authorized access … and is [a] widely used security tool that can prevent the interception of sensitive data, either while stored in files or while in transit across networks."[34]

43. The reporters' accusations turned out to be correct. "In a series of emails … Anker [] finally admitted its Eufy security cameras [were] *not* natively

[32] Sean Hollister, *Anker Finally Comes Clean About Its Eufy Security Cameras*, The Verge (Jan. 31, 2023) *available* https://www.theverge.com/23573362/anker-eufy-security-camera-answers-encryption (Feb. 1, 2024) (Emphasis added).

[33] Kyle Barr, *Eufy Finally Admits its "Local" Cameras Were Sending Unencrypted Streams, Claims It Will Do Better*, Gizmodo (Feb. 1, 2023) *available* https://gizmodo.com/eufy-local-security-camera-cloud-unencrypted-scandal-1850059207 (last accessed Oct. 23, 2023).

[34] Cisco, *What is Encryption?* available https://www.cisco.com/c/en/us/products/security/encryption-explained.html (last accessed Oct. 23, 2023).

end-to-end encrypted—they [could] and *did* produce unencrypted video streams from Eufy's web portal."[35]

44. In fact, Eufy's systems were so vulnerable that, despite "a Eufy Support representative['s] state[ment] that [facial] thumbnails [were] restricted by account logins[,]"[36] one security expert was easily able to hack into his own Eufy system—despite unplugging it—and "could pull up a thumbnail image of himself, an image of the feed shortly before he was visible, and—perhaps more concerning—ID numbers indicating his recognized face and his status as the camera owner."[37]

45. And, although Eufy has since hired "outside security and penetration testing companies to audit [its] practices,"[38] as referenced above, unsecured biometric identifiers stored on easily compromised systems—as Eufy did—is precisely the type of risk BIPA was enacted to protect the subject of a recording from.Indeed, the Illinois Legislature was motivated to enact BIPA to protect unauthorized disclosure of biometric identifiers because "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information." 740 ILCS 14/5(c). Accordingly, because "[b]iometrics [] are biologically unique to the individual [,] once compromised, the individual has no recourse, is at heightened risk for identify theft, and is likely to withdraw from biometric-facilitated transactions." *Id.*

46. Due to these concerns, BIPA provides, *inter alia*, that a private entity like Defendant may not obtain and/or possess an individual's biometric identifiers

---

[35] Sean Hollister, *supra* note 32.

[36] Kevin Purdy, *Eufy's "No Clouds" Cameras Upload Facial Thumbnails to AWS*, ARS Technica (Nov. 30, 2022) *available* https://arstechnica.com/gadgets/2022/11/eufys-no-clouds-cameras-upload-facial-thumbnails-to-aws/ (last accessed Oct. 23, 2023).

[37] *Id.*

[38] Sean Hollister, *supra* note 32.

unless it informs that person in writing that biometric identifiers will be collected or stored. *See* 740 ILCS 14/15(b).

47. Likewise, BIPA also requires that entities collecting biometric identifiers publish and make publicly available written retention schedules and guidelines for permanently destroying biometric identifiers collected. *See* 740 ILCS 14/15(c).

II. Illinois' Biometric Information Privacy Act

48. BIPA defines biometric identifiers as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10. (emphasis added).

49. Facial geometry is a permanent, unique biometric identifier associated only with a specific person. Collecting and storing a person's face geometry exposes them to serious and irreversible privacy risks. For example, if a device or database containing stored images of facial geometry is hacked, breached, or otherwise compromised, the person has no means by which they can prevent identity theft or unauthorized hacking of secure devices which use facial recognition to grant access.

50. Recognizing the need to protect citizens from these risks, Illinois enacted the Biometric Information Privacy Act, 740 ILCS 14/1, *et seq.* ("BIPA") in 2008, to regulate companies that collect and store biometric identifiers, such as facial geometry. *See* Illinois House Transcript, 2008 Reg. Sess. No. 276.

51. Accordingly, BIPA makes it unlawful for a company to, *inter alia*, "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers … unless it first:

1) informs the subject . . . in writing that a biometric identifier … is being collected or stored;

2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier … is being collected, stored, and used; and

> 3) receives a written release executed by the subject of the biometric identifier … or the subject's legally authorized representative."

740 ILCS 14/15(b).

52. Additionally, Section 15(a) requires that entities in possession of biometric identifiers publish a schedule detailing its retention and destruction plans concerning the biometric identifiers in its possession.

53. Section 15(a) of BIPA provides that:

> A private entity in possession of biometric identifiers … must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers … when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first.

740 ILCS 14/15(a).

54. As alleged below, Defendant's practices of collecting, storing, and using delivery drivers' biometric identifiers without informed written consent violated all three prongs of § 15(b) of BIPA. Furthermore, Defendant violates § 15(a) of BIPA by failing to publish and make publicly available any written policy regarding Defendant's schedule and guidelines for retaining and permanently destroying individuals' biometric identifiers.

III. Defendant Violates Illinois' Biometric Information Privacy Act

55. Unbeknownst to Plaintiffs, and in direct violation of § 15(b)(1) of BIPA, Defendant collected, scanned, and then indefinitely stored in an electronic database, Plaintiffs' biometric identifiers when Plaintiffs and Class Members made deliveries to the homes of Defendant's customers who used Defendant's security system. Each time Plaintiffs and Class Members made a delivery to Defendant's customers' homes, Defendant's cameras collected Plaintiffs' face and/or hand

geometry and stored the images of Plaintiffs' face and body geometry in an electronic database without ever informing Plaintiffs in writing that it was doing so.

56. Moreover, in direct violation of §§ 15(b)(2) and 15(b)(3) of BIPA, Defendant never informed Plaintiffs and Class Members who had their biometric identifiers collected, of the specific purpose and length of time for which their biometric identifiers would be collected, stored, and used, nor did Defendant ever obtain a written release.

57. Finally, and in direct violation of § 15(a) of BIPA, Defendant failed to publish policies for public access identifying its retention schedules or guidelines for permanently destroying any of these biometric identifiers.

CLASS ALLEGATIONS

58. Plaintiffs bring this matter on behalf of themselves and all similarly situated in the following class:

> **Illinois Class:** All natural persons in Illinois who are delivery drivers and who, when making deliveries, had their biometric identifiers collected, stored, and scanned by Eufy cameras and software from November 27, 2018, to present.

59. Excluded from the Class are: (1) any Judge or Magistrate presiding over this action and any members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which Defendant or its parent has a controlling interest and their current or former employees, officers, and directors; and (3) Plaintiff's counsel and Defendant's counsel.

60. The members of the Class are so numerous that joinder of all members is impracticable. While the exact number of Class members is unknown to Plaintiffs at this time, such information can be ascertained through appropriate discovery from records maintained by Defendant and its agents.

61. Plaintiffs reserve the right to expand, limit, modify, or amend the class definition, including the addition of one or more Subclasses, in connection with their

motion for class certification, or at any other time, based on, *inter alia*, changing circumstances and new facts obtained.

62. **Numerosity:** Class Members are so numerous that joinder of all members is impracticable. Plaintiffs believe that there are thousands of delivery drivers who are Class Members described above who have been damaged by Defendant's unlawful collecting, storing, and using of their biometric identifiers.

63. **Commonality and Predominance:** The questions of law and fact common to the class which predominate over any questions which may affect individual class members include, but are not limited to:

a. whether Defendant collected or otherwise obtained Plaintiffs' and the Class's biometric identifiers;

b. whether Defendant properly informed Plaintiffs and the Class that it collected, used, and stored their biometric identifiers;

c. whether Defendant obtained a written release (as defined by 740 ILCS 14/10) to collect, use, and store Plaintiffs' and the Class's biometric identifiers;

d. whether Defendant developed a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers when the initial purpose for collecting or obtaining such identifiers has been satisfied or within 3 years of their last interaction, whichever comes first;

e. whether Defendant destroyed Plaintiffs' and the Class's biometric identifiers once that information was no longer needed for the purpose for which it was originally collected; and

f. whether Defendant's violations of BIPA were committed intentionally, recklessly, or negligently.

64. **Typicality:** The claims of the named Plaintiffs are typical of the claims of the Class because the named Plaintiffs, like other members of the Class, made

deliveries to customer's homes and had their biometric identifiers collected, stored, and analyzed by Defendant's cameras and software without providing consent, nor did Defendant provide Plaintiffs and Class Members with written policy made publicly available establishing a schedule and procedure for permanently destroying Plaintiffs' and Class Members' biometric identifiers.

65. **Adequate Representation:** Plaintiffs have retained and are represented by qualified and competent counsel who are highly experienced in complex consumer class action litigation. Plaintiffs and their counsel are committed to vigorously prosecuting this class action. Neither Plaintiffs, nor their counsel, have any interest adverse to, or in conflict with, the interests of the absent members of the Class. Plaintiffs are able to fairly and adequately represent the interests of the Class. Plaintiffs have raised viable statutory claims of the type reasonably expected to be raised by members of the Class and will vigorously pursue those claims. If necessary, Plaintiffs may seek leave of this Court to amend this complaint to include additional Class Representatives to represent the Class or additional claims as may be appropriate.

66. **Superiority:** A class action is superior to other available methods for the fair and efficient adjudication of this controversy because individual litigation of the claims of all members of the Class is impracticable. Even if every member of the Class could afford to pursue individual litigation, the Court system could not. It would be unduly burdensome to the courts in which individual litigation of numerous cases would proceed. Individualized litigation would also present the potential for varying, inconsistent, or contradictory judgments, and would magnify the delay and expense to all parties and to the court system resulting in multiple trials of the same factual issues. By contrast, the maintenance of this action as a class action, with respect to some or all of the issues presented herein, presents fewer management difficulties, conserves the resources of the parties and of the court system and protects the rights of each member of the Class. Plaintiffs anticipate no

difficulty in the management of this action as a class action. Class-wide relief is essential to compel compliance with BIPA.

COUNT I
Violation of 740 ILCS 14/15(b)
(On Behalf of Plaintiffs and the Class)

67. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

68. BIPA makes it unlawful for any private entity to, among other things, "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers … unless it first: (1) informs the subject . . . in writing that a biometric identifier … is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier … is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or information. . ." 740 ILCS 14/15(b).

69. Defendant failed to comply with these BIPA mandates.

70. Fantasia Trading LLC is a limited liability company doing business as Eufy and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS 14/10.

71. Plaintiffs and Class Members are delivery drivers in Illinois who had their "biometric identifiers," including scans of face and hand geometry, collected, captured, received, or otherwise obtained by Eufy from video and/or images recorded by a Eufy device and scanned by Eufy software to differentiate between humans and non-human entrants on the camera-owner's property.

72. Plaintiffs and Class Members' face, body, and hand geometry was stored and mechanically measured to create numerical representations used as "face templates" that can be used to uniquely identify Plaintiffs and Class Members. *See* 740 ILCS 14/10.

73. Eufy systematically and automatically collected, captured, or otherwise obtained Plaintiffs' and Class Members' "biometric identifiers" (which it used to create and store uniquely identifying face geometry) without first obtaining signed written releases, as required by 740 ILCS 14/15(b)(3), from any of them.

74. Plaintiffs' and the Class's scans of face and/or hand geometry constitute "biometric identifiers." *See* 740 ILCS 14/10.

75. Defendant never informed Plaintiffs or members of the Class in writing that their biometric identifiers were being collected, captured, stored, and/or used, nor did Defendant inform Plaintiffs and members of the Class in writing of the length of time for which their biometric identifiers were being collected, stored, and used as required by 740 ILCS 14/15(b)(1)-(2).

76. By collecting, capturing, storing, and/or using Plaintiffs' and members of the Class's biometric identifiers as described herein, Defendant violated Plaintiffs' and the Class's right to privacy in their biometric identifiers as set forth in BIPA. *See* 740 ILCS 14/1, *et seq.*

77. And while Plaintiffs and members of the Class are not required to plead that Defendant can link these identifiers back to Plaintiff and Class Members, Defendant is nonetheless able to do so. This is because most people have Facebook, Twitter, Snapchat, or other social media accounts bearing their real-life names and photos. Those real-life names and photos are publicly available to allow other unconnected people to find them. Defendant is capable of employing the very same facial recognition technology used in its cameras and base stations on someone's public facing social media profile to match that individual's biometric identifiers collected from their public online photos to their biometric identifiers collected by its cameras and base station during a home visit. As such, Defendant's human recognition feature is capable identifying an individual.

78. On behalf of themselves and the Class, Plaintiffs seek: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interest of

Plaintiffs and the Class by requiring Eufy comply with BIPA's requirements for the collection, storage, and use of "biometric identifiers" as described herein; (3) statutory damages of $1,000.00 pursuant to 740 ILCS 14/20 for each negligent violation of BIPA committed by Eufy; (4) statutory damages of $5,000.00 pursuant to 740 ILCS 14/20 for each intentional or reckless violation of BIPA committed by Eufy; and (5) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

COUNT II
Violation of 740 ILCS 14/15(a)
(On Behalf of Plaintiffs and the Class)

79. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

80. BIPA mandates that companies in possession of biometric data establish and maintain a satisfactory biometric data retention and deletion policy. Specifically, those companies must: (i) make publicly available a written policy establishing a retention schedule and guidelines for permanent deletion of biometric data (at most three years after the company's last interaction with the individual); and (ii) actually adhere to that retention schedule and actually delete the biometric identifiers. *See* 740 ILCS 14/15(a).

81. Defendant failed to comply with these BIPA mandates.

82. Defendant is a limited liability company and thus qualifies as a "private entity" under BIPA. *See* 740 ILCS 14/10.

83. Plaintiffs are individuals who had their "biometric identifiers" captured and/or collected by Defendant, as explained in detail above. *See* 740 ILCS 14/10.

84. Plaintiffs' biometric identifiers consisted of scans of face geometry, as defined by BIPA. *See* 740 ILCS 14/10.

85. Defendant failed to provide a publicly available retention schedule or guidelines for permanently destroying Plaintiffs' biometric identifiers as specified by BIPA. *See* 740 ILCS 14/15(a).

86. On behalf of themselves and the Class, Plaintiffs seek: (1) declaratory relief; (2) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the Class by requiring Defendant to comply with BIPA's requirements for the collecting, storing, and using biometric identifiers as described herein; (3) statutory damages of $5,000 for each intentional and/or reckless violation of BIPA pursuant to 740 ILCS 14/20(2) or, in the alternative, statutory damages of $1,000 for each negligent violation of BIPA pursuant to 740 ILCS 14/20(1); and (4) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, seek judgement against Defendants as follows:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiffs as representatives of the Class, and appointing their counsel as Class Counsel of the Class;

B. Declaring that Defendant's actions, as set out above, violate BIPA, 740 ILCS 14/1, *et seq.*, with respect to Plaintiffs and Class Members;

C. Awarding statutory damages to Plaintiffs and Class Members of $1,000.00 pursuant to 740 ILCS 14/20(1) for each violation of BIPA committed negligently, and $5,000.00 pursuant to 740 ILCS 14/20(2) for each violation of BIPA committed intentionally or recklessly;

D. Awarding injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and members of the Class, including *inter alia*, an order requiring Defendant to collect, store, and use biometric identifiers in compliance with BIPA;

E. Awarding Plaintiffs and the Class their reasonable litigation expenses and attorneys' fees pursuant to BIPA;

F. Awarding Plaintiffs and the Class pre- and post-judgment interest, to the extent allowable;

G. Awarding Plaintiffs and the Class such other and further relief as equity and justice may require.

JURY TRIAL DEMANDED

Under Federal Rule of Civil Procedure 38, Plaintiffs, individually and on behalf of the members of the Class, exercise their right under the Seventh Amendment to the United States Constitution and demand a trial by jury.

Dated: February 12, 2024

Respectfully submitted,

BURSOR & FISHER, P.A.

By: /s/ *L. Timothy Fisher*
L. Timothy Fisher

L. Timothy Fisher (State Bar No. 191626)
Stefan Bogdanovich (State Bar No. 324525)
1990 North California Blvd., Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: ltfisher@bursor.com
sbogdanovich@bursor.com

Attorneys for Plaintiffs